WHA GROUP

Standard

AI Management Standard

Document Properties	
Document Number	WHACG-ICT-STND-0008
Softcopy Location	CDMS / WHA SharePoint
Owner Division	IT Department
Owner Department	IT Department
Version Number	v1.1.0 (Approved Final)
Release Date	28 Aug 2026

Document Approval

Approver	Jareeporn Jarukornsakul (Chairman of the Executive Committee and Group Chief Executive Officer) Pajongwit Pongsivapai (Chief Executive Officer – WHA Industrial Development) Akarin Prathuangsit (Chief Executive Officer – WHA Utilities and Power) Nunsilp Janvarin (Acting Chief Executive Officer – WHA Digital)
Reviewer	Nunsilp Janvarin (Chief Technology Officer) Nattapong Kanyanutcharat (Director – IT Department) Patcharin Tongaree (Data and AI Deputy Director – IT Department)
Owner	Soros Sottitavorn (Infrastructure and Cybersecurity Deputy Director - IT Department)

Document Control

Document Changes:

The following table presents the change record of this document.

Version	Approval date	Document owner	Change(s)
1.1.0	28 Aug 2026	Soros Sottitavorn – Infrastructure and Cybersecurity Deputy Director	Update content 3.4.1 about maintain a low ecological footprint
1.0.0	11 Aug 2026	Soros Sottitavorn – Infrastructure and Cybersecurity Deputy Director	First version.

Authors:

The following persons are the authors who drafted this document.

Name - Surname	Position
Soros Sottitavorn	Infrastructure and Cybersecurity Deputy Director - IT Department

Reviewers:

In addition to the main reviewers, the following persons have also reviewed this document.

Name - Surname	Position
Nunsilp Janvarin	Chief Technology Officer
Nattapong Kanyanutcharat	Director – IT Department
Patcharin Tongaree	Data and AI Deputy Director – IT Department

Approvers:

In addition to the main approvers, the following persons have also approved this document.

Name - Surname	Position
Jareeporn Jarukornsakul	Chairman of the Executive Committee and Group Chief Executive Officer
Pajongwit Pongsivapai	Chief Executive Officer – WHA Industrial Development
Akarin Prathuangsit	Chief Executive Officer – WHA Utilities and Power
Nunsilp Janvarin	Acting Chief Executive Officer – WHA Digital

Table of Contents

1) Introduction

In an era where Artificial Intelligence (AI) plays an important role in business operations and innovation, the organization needs a clear approach for AI management to ensure that AI is used efficiently, transparently, ethically, and securely. This AI Management Standard has therefore been established as an operational framework aligned with the organization's strategy and international standards such as ISO/IEC 42001.

Although the use of AI can support business development and create added value for the organization, it also introduces risks that must be carefully managed, including risks related to data accuracy, fairness, security, and personal data protection. This standard therefore focuses on the responsible and ethical use of AI by establishing key principles such as transparency, fairness, cybersecurity and information security, and compliance with applicable laws. The standard covers secure and auditable processes, as well as continuous assessment and improvement, to ensure that AI use strengthens competitiveness, supports sustainable organizational growth, and builds confidence among stakeholders.

The use of AI technology without proper governance and accountability may cause negative impacts on individuals, the organization, society, and the country, such as:

1) Misinformation and disinformation that may cause misunderstanding
2) Factually inaccurate content or confabulated information
3) Dangerous or violent recommendations
4) Content that may affect data privacy
5) Content involving sensitive matters or ethical concerns
6) Incomplete, inaccurate, or manipulated information that affects information integrity
7) Bias, division, and discrimination against individuals or groups of individuals
8) Personal data leakage
9) Intellectual property infringement
10) Information security risks
11) Other potential impacts arising from AI technology or similar technologies

Therefore, this AI Management Standard has been established to ensure that the use of Artificial Intelligence (AI) technology in WHA Group's activities is efficient, transparent, aligned with good governance principles, and compliant with applicable laws.

2) AI Management Objectives

This standard has been developed to provide key content that can be used as guidance for training, awareness building, understanding the consequences of non-compliance, and examples of appropriate and inappropriate behaviors when using Artificial Intelligence (AI) technology, including AI applications or services recommended by the organization. It aims to enable employees, workers, personnel, and contractors of the organization to use AI technology appropriately, responsibly, safely, and efficiently, while preventing risks arising from inappropriate use. The organization has therefore defined the following objectives:

1. To provide employees, workers, personnel, and contractors with practical guidance for using AI technology correctly, appropriately, and efficiently.
2. To ensure that the use and development of AI is responsible, secure, ethical, and compliant with applicable laws, rules, regulations, announcements, requirements, and other relevant obligations, while respecting data privacy, protecting the cybersecurity of systems, and preventing risks arising from misuse of AI or biased outcomes that may affect individuals, the organization, society, or the country.
3. To promote awareness and understanding of responsible and careful AI use, enabling appropriate use in accordance with the organization's defined guidelines.

3) AI Management Standard

Standard Content and Implementation

3.1) Policies related to AI

Objective: To establish direction and support for responsible, transparent AI management that aligns with business requirements.

The organization has established the Cybersecurity, Information Security & Privacy and AI Governance Policy to set the direction and governance approach for AI management, and has developed this AI Management Standard in alignment with international standard requirements.

3.1.1) AI Management Standard

This AI Management Standard has been established for the responsible development or use of AI systems.

Implementation Guidelines

This standard consists of the following:

- Business strategy
- Organizational values and culture
- The organization's risk appetite
- Risk level of AI systems
- Legal requirements applicable to the organization, including relevant contractual obligations
- Organizational context
- Impacts of AI systems on stakeholders

This standard covers the following content:

- AI principles that provide guidance for activities related to AI
- Processes for managing deviations and exceptions to the AI policy and standard

This standard should consider defining organization-specific topics as necessary, or refer to other policies related to those topics, for example:

- AI resources and assets
- Assessment of AI system impacts
- AI system development

In addition, this standard also covers system development, procurement, and the use of AI systems.

3.1.2) Alignment with other organizational policies

The organization shall define other policies related to the AI policy and/or AI management standard and apply them to support the organization's objectives for AI systems.

Implementation Guidelines

The scope of AI overlaps with many other areas, such as quality, cybersecurity and information security, safety, and privacy. Therefore, the organization should conduct a detailed analysis to identify overlapping policies and update the relevant policies accordingly, or incorporate AI-related content or requirements into those policies.

3.1.3) Review of the AI policy/standard

The AI policy and/or AI management standard shall be reviewed at least once a year, or additionally as necessary, to ensure continued suitability, adequacy, and effectiveness.

Implementation Guidelines

The AI Governance Steering Committee should be responsible for developing, reviewing, and evaluating the AI policy and standard, including all relevant components of the policy and standard. The review should include an assessment of opportunities to improve organizational policies and the approach for managing AI systems, so that the organization can respond to changes in the organizational environment, business conditions, legal requirements, or technical environment.

3.2) Internal organization

Objective: To define internal responsibilities and support the organization's approach to deploying, using, and managing the organization's AI systems.

3.2.1) AI roles and responsibilities

Roles and responsibilities for AI shall be defined and assigned to relevant parties as necessary for the organization.

Implementation Guidelines

Defining the roles and responsibilities of relevant departments or personnel is important for ensuring accountability across the organization according to assigned roles related to AI systems throughout the AI system life cycle. The assignment of roles and responsibilities should be based on the policy and standard, objectives, and AI-related risks to ensure that all relevant departments are covered. The organization may prioritize these roles and responsibilities as appropriate.

The organization has established an AI Governance Steering Committee as follows:

1. The organizational structure of the AI Governance Steering Committee is shown in the figure below.

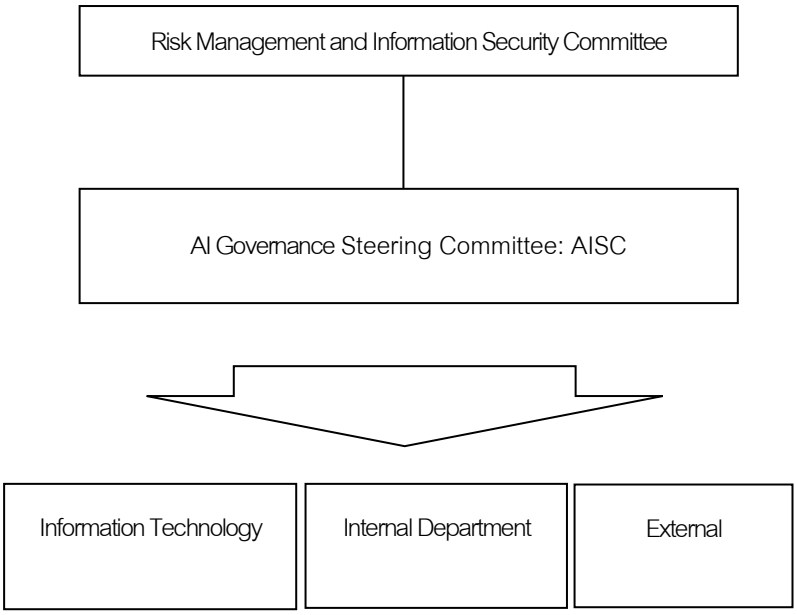

Figure 1: Organizational structure of the AI Governance Steering Committee

2. The AI Governance Steering Committee consists of executives from the following departments:

(1) Chief Technology Officer	Committee Chairperson / AIMR
(2) AI Manager	Secretary / AIMA
(3) Information Technology Specialist	Committee Member
(4) Operations Specialist	Committee Member
(5) Human Resources Specialist	Committee Member
(6) Business Development Specialist	Committee Member
(7) Finance Specialist	Committee Member
(8) Data Protection Officer	Committee Member

Each specialist may either be appointed by the relevant division's executive or automatically serve as the director of that division.

The Risk Management and Information Security Committee has defined the roles, duties, and responsibilities of relevant parties in accordance with the AI Governance Steering Committee structure as follows:

3.2.1.1) Roles and Responsibilities of the AI Governance Steering Committee

1) Define the organization's AI management objectives.
2) Review, revise, and establish the AI management standard.
3) Define risk and impact acceptance criteria and/or acceptable risk and impact levels, and consider key risk assessment results and risk treatment plans of the organization, and report to the Risk Management and Information Security Committee for approval.
4) Review and endorse projects related to AI.
5) Plan, review, and manage the organization's risks and impacts related to AI.
6) Review, monitor, and evaluate continuity plans for the use and development of AI.
7) Plan communication and training for all personnel across the organization to understand the responsible, correct, and appropriate use and development of AI.
8) Support communication to ensure that all employees recognize the importance of responsible AI use and development, and comply with the AI management policy and/or standard and related AIMS documents.
9) Support the provision of knowledge to employees and relevant external parties so that they understand and can comply with the AI management policy and/or standard and related AIMS documents, including appropriately monitoring compliance by employees and relevant external parties.
10) Gather facts, summarize, and provide opinions regarding violations of the AI management policy and/or standard and related AIMS documents, and present such information to the relevant units.
11) Provide support for the resources necessary to establish, operate, review, and improve the AIMS.
12) Participate in meetings to review AIMS operations to ensure that the organization's AIMS remains suitable, adequate, and effective, including considering opportunities for the continual improvement of the AIMS.

3.2.1.2) Roles and Responsibilities of AIMR / AIMA

1) Oversee the update and revision of the AI policy, standard and related AIMS documents to ensure they remain appropriate for changes, aligned with ISO/IEC 42001, and consistent with recommendations from the AI Governance Steering Committee.
2) Communicate to all employees their roles and responsibilities for complying with the policy and related AIMS documents.
3) Monitor the organization's operations to ensure compliance with the requirements defined in AIMS documents.
4) Provide advice and guidance on information security and the implementation of relevant policies to personnel within the organization.

5) Engage external consultants or experts to provide consultation or training when necessary.
6) Oversee changes occurring within the organization, and coordinate appropriate assessment, mitigation, and control of risks arising from such changes.
7) Oversee the measurement of effectiveness of AIMS processes and controls.
8) Coordinate and support the internal AIMS audit to ensure it is conducted appropriately.
9) Oversee corrective and preventive actions for AIMS nonconformities, including appropriately follow-up and reviewing the effectiveness of such actions.
10) Coordinate and support the holding of meetings to review AIMS operations by the AISC at least once every quarter, and follow up on actions arising from meeting resolutions
11) Report the operational results of the AIMS, comprising all defined management standards, to the AISC at least once every quarter.
12) Coordinate and identify appropriate measures to control and manage issues in the event of an AI-related incident occurring within the organization, and report to the Incident Response Team, or report to the DPO in cases involving personal data.

3.2.1.3) Information Technology Department

The Information Technology Department is established to prevent organizational damage arising from AI, such as misuse of AI, and to ensure that AI-related activities are aligned with the organization's business objectives.

3.2.1.3.1) Chief Technology Officer (CTO)

(1) Chair the AI Governance Steering Committee and be responsible for AI management, including leading all AI-related activities within the organization.
(2) Define AI management objectives, policies, and standards in alignment with the organization's strategic plan.
(3) Present AI operational plans, policies, budgets, manpower requirements, and AI implementation plans for approval by the Group Chief Executive Officer (Group CEO) and Chief Executive Officer (CEO), while ensuring awareness of the importance of AI management.
(4) Analyze and manage AI-related risks, including assessing appropriate options for addressing AI risks.
(5) Manage the development of AI management policies to ensure the stability of AI systems, accuracy, and confidentiality of information.
(6) Manage the use of AI by preventing, reviewing, and monitoring the development and deployment of AI.
(7) Communicate and maintain relationships with partners, organizations, or external parties related to AI in both the public and private sectors.

(8) Review and approve AI management standards, procedures, and organizational guidelines to ensure they are appropriate to the importance of business processes.

(9) Establish the AI management team to enable effective management and operations.

3.2.1.3.2) AI Manager

(1) Report directly to the CTO on all AI-related operations, including regularly reporting AI management progress to the CTO.

(2) Design AI management standards, procedures, and organizational guidelines appropriate to the importance of business processes.

(3) Review all standards and procedures related to AI management.

(4) Act as an AI advisor to the CTO to support appropriate AI risk analysis and management and provide AI knowledge to other departments.

(5) Ensure that the defined processes and controls are implemented sustainably.

(6) Manage the use of AI and plan AI management activities across relevant areas.

(7) Review and monitor AI-related communications.

(8) Maintain preparedness for AI-related situations and continuously learn new developments in AI.

(9) Control and manage the AI team so that it can operate effectively when AI-related incidents occur within the organization, such as leakage of personal data used in AI systems.

3.2.1.3.3) AI Development Team

(1) Oversee AI systems to ensure smooth operation.

(2) Prevent, review, and monitor AI systems to ensure correct operation and prevent data leakage.

(3) Respond to AI-related incidents within the organization, such as leakage of personal data used in AI systems.

(4) Provide consultation and support during AI system development and during awareness, training, and user education activities related to AI use.

3.2.1.4) Internal Departments

Internal departments refer to all employees of the organization who are involved with AI in any way. They can be classified as follows:

3.2.1.4.1) Head of Division / Department Head

Responsibilities are as follows:

(1) Provide guidance to employees under their supervision and emphasize the importance of AI use and the need to appropriately protect information for business operations.

(2) Make business decisions in alignment with the AI policy or AI Management Standard.

3.2.1.4.2) Data / AI Owner

Responsibilities are as follows:

(1) Own and fully control their data/AI in accordance with applicable laws and other relevant operational requirements.

(2) Define, manage, and control the creation, processing, dissemination, and disposal of data/AI.

3.2.1.4.3) Employees

All employees of the organization who are involved with AI in any way have the following responsibilities:

(1) Strictly comply with the AI Management Standard.

(2) Maintain the confidentiality of organizational information, do not use the organization's confidential information with AI services outside the organization, and do not disclose their own system passwords.

(3) Protect and maintain the privacy of personal information.

(4) Report AI-related incidents or issues, including information security issues, when an event related to AI use occurs.

(5) Use the organization's AI, data, and AI assets responsibly, ethically, transparently, and securely, and use AI only for work within their responsibilities or as authorized.

The following internal departments will provide support as follows:

3.2.1.4.4) Human Resources

Responsibilities are as follows:

(1) Provide advice and consultation on policies and requirements related to employment, performance evaluation, relevant human resources matters, and guidance on personal data.

(2) Provide management support for maintaining necessary records to comply with laws, regulations, and internal policies related to human resources, which may be necessary for controlling system access and reviewing access to AI systems.

3.2.1.4.5) Legal: Provide legal support and guidance to ensure the organization's business operations comply with applicable laws, regulations, rules, and requirements.

3.2.1.4.6) Internal Audit

(1) Plan, coordinate, and conduct internal audits for the AI Management System (AIMS).

(2) Report internal audit results for the AI Management System (AIMS) and provide improvement recommendations to relevant parties.

(3) Follow up and review corrective or preventive actions for deficiencies identified from internal audits of the AI Management System (AIMS).

3.2.1.5) External Parties

External parties are third parties who work within the organization or perform work for the organization and are involved in the use of the organization's data or AI assets, such as service providers, vendors, system contractors, or authorized parties. They have the same responsibilities as the organization's employees.

3.2.2) Reporting of concerns

The organization shall establish and implement a process for reporting concerns regarding organizational roles related to AI systems throughout the system life cycle, including a process that enables users, affected individuals, and relevant third parties to report concerns, request human review, and, where appropriate, appeal or contest AI-generated decisions or outcomes that may adversely affect them.

Implementation Guidelines

The mechanism for reporting concerns regarding organizational roles related to AI systems should cover the following:

- Options for confidential reporting and/or anonymous reporting
- Reporting to organizational personnel or contracted personnel, as applicable
- Availability of appropriately qualified personnel
- Defined conditions for investigation and authority to take necessary actions
- A mechanism for timely reporting to management
- A mechanism to prevent retaliation against individuals involved in reporting and investigations, including where reports are confidential or anonymous
- Defined appropriate response timelines for concerns that have been reported
- A documented process that enables users, affected individuals, and relevant third parties to request human review of AI-generated decisions or outcomes that may significantly affect them
- A documented appeals process for contesting AI-generated decisions or outcomes, including defined responsibilities, review procedures, and decision-making authority
- Authority for qualified personnel to investigate, override, modify, or reverse AI-generated decisions where appropriate
- Communication of the outcome of investigations or appeals to the reporting party, where permitted by applicable laws and organizational policies
- Recording and monitoring reported concerns and appeal outcomes to support continual improvement of AI systems, governance processes, and risk management

3.3) Resources for AI systems

Objective: To enable the organization to define responsibilities for resources, including AI system components and assets required to manage potential risks and impacts.

3.3.1) Resource documentation

The organization shall identify and document the resources required for activities related to AI systems throughout the system life cycle, including other activities related to the organization's AI systems.

Implementation Guidelines

AI system resource documentation is important for understanding the risks and impacts of AI systems, both positive and negative, on individuals, groups of individuals, or both, as well as on relevant society.

AI system resources may include the following:

- AI system components
- Data resources, including data used at each stage of system development
- Tooling resources, including models, algorithms, and other tools used
- System and computing resources, including hardware used for model development and data storage media
- Human resources, including personnel with expertise in relevant areas throughout the AI system life cycle

Resources may be owned by the organization or may be provided by customers or external service providers.

3.3.2) Data resources

The organization shall document the data resources used by AI systems as part of AI system resource documentation.

Implementation Guidelines

Documentation related to data used by AI systems may cover the following content:

- Data sources
- Date on which the data was last updated
- Type of data, such as training data, test data, and production data
- Data naming
- Intended use of the data
- Data quality
- Data retention and disposal period
- Bias issues related to the data
- Data preparation

3.3.3) Tooling resources

The organization shall document the tooling resources used by AI systems as part of AI system resource documentation.

Implementation Guidelines

Tooling resources for AI systems and machine learning may include the following resources:

- Types of machine learning algorithms and models
- Tools or processes for data preprocessing
- Methods for tuning machine learning algorithms and models
- Evaluation methods
- Tools supporting model development
- Software and hardware used for system design, development, and deployment

3.3.4) System and computing resources

The organization shall document the system and computing resources required for AI systems as part of AI system resource documentation.

Implementation Guidelines

Information related to AI system and computing resources may include the following:

- Resource requirements for the AI system to be used
- Location of system and computing resources for the AI system
- Processing resources used by the AI system, including network and storage resources
- Impacts of hardware used for AI system operations, such as environmental impacts from hardware use or manufacturing, or costs associated with hardware use

3.3.5) Human resources

The organization shall document the human resources and required competencies necessary for AI system development, deployment, operation, modification, maintenance, transfer, decommissioning, validation, and integration into the organization's systems.

Implementation Guidelines

The organization should document the human resources and competencies required for system development, deployment, operation, administration, modification, maintenance, transfer, decommissioning, validation, and integration of AI systems into the organization's systems.

Required human resources may include the following:

- Data scientists
- Roles related to human control and oversight

- Experts related to AI system trustworthiness, such as safety, cybersecurity and information security, and privacy experts
- Researchers, specialists, and professionals in relevant fields related to AI systems

3.4) Assessing impacts of AI systems

Objective: To assess the impacts of AI systems on individuals, groups of individuals, or both, and on society affected by AI systems throughout the system life cycle.

3.4.1) AI system impact assessment process

The organization shall define a process for assessing the potential impacts of AI systems on individuals, groups of individuals, or both, and on society that may be affected by the organization's AI systems throughout the system life cycle. Furthermore, the organization shall require AI models and data centers supporting high compute intensity AI systems, whether owned by the organization or provided by third-party service providers, to maintain a low ecological footprint by establishing verifiable measures to minimize their environmental impacts. Such measures shall cover measuring and reducing energy consumption and carbon emissions, promoting techniques to optimize system performance, requiring the use of energy-efficient infrastructure, and promoting the use of renewable energy in operations related to AI systems.

Implementation Guidelines

Because AI systems can affect individuals, groups of individuals, or both, and society, organizations that use such systems should consider the intended purpose of AI system use and assess the potential impacts of those AI systems on such groups.

The organization should consider whether the AI system has impacts on the following areas:

- Legal impacts
- Impacts on individuals' lives
- Physical or psychological well-being of individuals
- Human rights
- Society

The impact assessment procedures should cover the following:

- Situations that require an impact assessment, including:
  - The purpose and context of AI use, or significant changes to the purpose and context of use
  - The complexity of AI technology and the level of automation of the AI system in use, or significant changes to the technology

- The sensitivity of the types and sources of data used by the AI system for processing, or significant changes to such data types and sources

- Elements of the AI system impact assessment process, which should cover the following:
  - Identifying sources or events that create impacts
  - Analyzing likelihood and impact
  - Evaluating impacts
  - Managing impacts, such as applying risk mitigation measures
  - Documenting impact assessment results
  - Reporting and communicating results to relevant parties
- Parties responsible for conducting the impact assessment
- Use of impact assessment results, such as using them to control system design or operation, or to require review and approval before deployment
- Individuals and society that may be affected

Impact assessments may consider these factors, such as data used for AI system development, technology used by the AI system, and system functionality.

3.4.2) Documentation of AI system impact assessments

The organization shall document the results of AI system impact assessments and retain the documentation for the period defined by the organization.

Implementation Guidelines

AI system impact assessment documentation should be communicated to users and relevant stakeholders.

AI system impact assessments should be retained for the defined retention period and updated as necessary.

The retention period for AI system impact assessment documentation shall follow the organization's document retention policy, applicable legal requirements, or other obligations with which the organization must comply.

The organization should consider documenting the following topics:

- The intended purpose of the AI system
- Reasonably foreseeable misuse of the AI system
- Positive and negative impacts of the AI system on individuals, groups of individuals, or both, and on society
- Foreseeable failures, potential impacts of such failures, and measures necessary to mitigate those impacts
- Relevant groups of individuals for whom the AI system is used
- Complexity of the AI system
- Human roles related to the system, including human control and oversight

- Processes and tools necessary to avoid negative impacts
- Availability of personnel with diverse skills

3.4.3) Assessing AI system impact on individuals or groups of individuals

The organization shall regularly assess and document the potential impacts of deployed AI systems on individuals or groups of individuals throughout the system life cycle.

Implementation Guidelines

When assessing impacts on individuals, groups of individuals, or both, and on society, the organization shall consider its AI governance principles, policies, and objectives.

Individuals who use AI systems, or whose personal data is processed by AI systems, may have expectations regarding the trustworthiness of those AI systems. In particular, special safeguards for certain groups of individuals, such as children, persons with disabilities, and elderly persons, should be considered. The organization shall consider and assess these needs and expectations and address them as part of the AI system impact assessment.

Impact assessments may cover the following areas:

- Fairness and equity
- Accountability
- Transparency and explainability of system operation
- Cybersecurity, information security, and data privacy
- Safety and health
- Financial impacts
- Accessibility
- Human rights

3.4.4) Assessing societal impacts of AI systems

The organization shall regularly assess and document the potential societal impacts of deployed AI systems throughout the system life cycle.

Implementation Guidelines

Societal impacts may vary depending on the context and type of AI system used by the organization. The impacts of AI systems may be both beneficial and harmful.

Examples of these impacts include the following:

- Environmental sustainability, such as impacts on natural resources and greenhouse gas emissions
- Economy, including access to financial services, employment opportunities, and taxation
- National governance, including legal processes, politically motivated disinformation, national security, and the criminal justice system

- Health and safety, including access to healthcare services, disease diagnosis and treatment, and physical and psychological harm
- Norms, traditions, culture, and values, including misinformation or disinformation created by malicious actors that may lead to bias or harm against individuals, groups of individuals, or both, and society

Where an AI project or tool is intended to create societal impact or support sustainability outcomes, the organization should define measurable sustainability objectives and indicators, assess both positive and negative impacts arising from the use of AI, periodically monitor performance, and use the assessment results to improve AI systems, sustainability initiatives, and organizational decision-making, including reporting such outcomes to management and stakeholders as appropriate.

3.5) AI system life cycle

3.5.1) Management guidance for AI system development

Objective: To identify and document objectives and implement processes for responsible AI system design and development.

Note: The organization's responsible approach covers activities that consider the risks and impacts affecting stakeholders of AI systems. The organization must demonstrate accountability to prevent risks to such stakeholders by taking appropriate actions. This approach is primarily considered from defining the objectives of the AI system, specifying system requirements, analyzing and designing the system, developing the system, deploying the system, operating the system, monitoring and tracking system performance, and maintaining the system. All of these stages must consider the risks and impacts that may affect stakeholders.

3.5.1.1) Objectives for responsible development of AI system

The organization shall identify and document objectives to guide the responsible development of AI systems, use those objectives to support system development decisions, and define measures to achieve those objectives throughout the AI system life cycle.

Implementation Guidelines

The organization shall define objectives (see section 3.5.2) that affect the AI system design and development process. The following topics may be used as objectives for AI system development:

- Fairness and equity
- Accountability
- Transparency and explainability of system operation
- Cybersecurity, information security, and data privacy
- Safety and health

- Financial impacts
- Accessibility
- Human rights

If the organization defines these topics as objectives for AI system development, the organization shall consider and implement necessary measures at every stage of the development process, such as system requirements definition, data acquisition, data preparation, model training, and system validation, to achieve the defined objectives.

3.5.1.2) **Processes for responsible AI system design and development**

The organization shall define and document processes for responsible AI system design and development.

Implementation Guidelines

The responsible system development process should cover the following topics:

- Each step in the development process that forms part of the system development life cycle
- System testing steps, including testing requirements and testing methods used
- Human control and oversight, including necessary processes and tools, particularly where the AI system may have an impact on individuals
- Impact assessment steps
- System training steps and expectations, including what data should be used for training and the consideration and approval of data obtained from external service providers
- Required specialized expertise
- Training for AI system developers
- Criteria for system deployment
- Approval and sign-off at each stage of system development
- System change management

3.5.2) AI system life cycle

Objective: To define the criteria and requirements for each stage of the AI system life cycle.

3.5.2.1) **AI system requirements and specification**

The organization shall identify and document AI system requirements, whether for new systems or enhancements to existing systems.

Implementation Guidelines

The organization should prepare documentation describing the rationale and necessity for developing the AI system and the objectives of the development. Factors to be considered and documented should include the following:

- The rationale and necessity for developing the AI system, such as business requirements, customer requirements, or government policy
- Methods for training the system model
- Alignment with requirements related to system data, such as system data quality requirements
- Requirements related to the AI system should be defined and cover the full AI system development life cycle. These requirements should be reviewed and updated as necessary, such as when there are changes to the originally defined requirements.

3.5.2.2) **Documentation of AI system design and development**

The organization shall document the design and development of AI systems in alignment with the organization's objectives, defined system requirements, and criteria specified in the system requirements documentation.

Implementation Guidelines

AI system design options may include the following:

- Machine learning approaches, such as supervised machine learning and unsupervised machine learning
- Machine learning algorithms and models used
- Model training methods and data quality issues related to the training data
- Model evaluation and improvement
- Hardware and software components
- Cybersecurity and information security threats
- AI-specific threats, such as data poisoning attacks, where abnormal or malicious data is introduced into the AI system and may cause the AI model to generate incorrect outputs or reduce overall system performance
- System user interface
- Methods by which users can interact with the system
- System integrations and interfaces
- Migration of the system to other platforms

The system design process may be reviewed and refined periodically to achieve the design that best fits the organization. Design documentation should be kept up to date, and system architecture information should be included as part of the system design.

3.5.2.3) **AI system verification and validation**

The organization shall define and document the necessary measures for AI system verification and validation, including the relevant criteria for those measures.

Implementation Guidelines

Measures used to validate system performance may cover the following:

- Methods and tools used for system testing
- Selection of data used for system testing
- Coverage of data used for system testing within the intended scope of use
- System acceptance criteria requirements for deployment

The organization should define and document system evaluation criteria covering the following:

- Plans for evaluating AI system components and the overall AI system, covering relevant system risks that may affect individuals, groups of individuals, or both, and society
- The system evaluation plan may consider the following:
  - System trustworthiness requirements, including acceptable error tolerance criteria
  - System safety requirements, including acceptable error tolerance criteria
  - Objectives for responsible development and use of the AI system
  - Factors related to system use
  - Intended system use
- Evaluation methods and metrics for assessing whether relevant stakeholders can correctly interpret AI system outputs
- System acceptance criteria for cases where the system does not achieve the defined target performance level, and mechanisms for performance improvement

The AI system should be evaluated against the defined system evaluation criteria.

3.5.2.4) **AI system deployment**

The organization shall prepare a deployment plan and assess whether the requirements related to the AI system are fulfilled before deployment.

Implementation Guidelines

An AI system may be developed in one environment and deployed in other environments. However, the organization shall carefully consider deployment in environments that differ from the development environment.

The organization should define deployment requirements that must be fulfilled before releasing the system into operation. Such requirements should cover measures used to validate system performance, performance indicators, user acceptance testing, and management approval and sign-off.

The deployment plan should also consider the perspectives of relevant stakeholders and the potential impacts on those groups.

3.5.2.5) **AI system operation and monitoring**

The organization shall define and document activities related to the ongoing operation of AI systems. At a minimum, this shall include system and performance monitoring, system repair, system improvement, and system support.

Implementation Guidelines

AI system operation and monitoring activities may cover the following:

- Monitoring system operation and performance, including errors and failures, whether the system operates as expected by stakeholders, the success rate of issue resolution, whether the system achieves the intended outcomes, the system confidence level, whether the system operates in accordance with customer requirements, and whether the system complies with applicable legal requirements.
- Monitoring whether system performance improves over time, such as through machine learning where data and outputs are used for further model training. In cases of continuous learning, the organization shall monitor system performance to ensure that it remains aligned with the system design objectives and continues to work effectively with the intended data. The organization should also implement mechanisms to monitor whether system performance is declining and correct such cases, such as detecting where changes in data distribution occur (data drift) or where the model objective or target changes (concept drift), or where degradation of AI models over time occurs, which may affect system performance.
- Improving or correcting the system so that it can respond to errors, failures, nonconformity with customer expectations or requirements, and noncompliance with applicable legal requirements.
- The organization should establish processes to respond to and resolve identified errors and failures by improving or correcting the system so that it performs more effectively and remains aligned with customer requirements and applicable legal requirements.
- Improving or correcting the system as a result of changes in system use, related operational activities, or system functions. The organization should have procedures to manage such changes to the system and communicate them to relevant users.
- Support related to the system may be provided internally, externally, or both, depending on the organization's needs and the method used to acquire the system. The support process should cover how users can request assistance, how system-related issues are resolved, including system unavailability, reporting channels for such issues, service level agreements, and related performance indicators.

- If AI system is being used for purposes other than those defined during system design and development, or is being used in an unexpected manner, the appropriateness of such use should be reassessed.
- AI-specific threats should be identified and managed, such as data poisoning, model stealing, and model inversion attacks.

3.5.2.6) **AI system technical documentation**

The organization shall define and prepare the technical documentation of AI systems required for each group of stakeholders, such as users, partners, supervisors, and other relevant parties, and shall provide the documentation in a format appropriate for those stakeholders.

Implementation Guidelines

AI system technical documentation may cover the following:

- A general description of the AI system, including the intended purpose of use
- Instructions or user manuals
- Technical assumptions related to system use, such as the operating environment
- Technical limitations of the system, such as acceptable system error rates, accuracy, and reliability
- System monitoring capabilities and functions

The components of technical documentation may include the following:

- System design details
- System architecture
- System design options
- Quality measures applied during system development
- Data used during system development
- Quality measures for the data used
- Management activities, such as risk management
- Documentation of system validation results
- Changes made to the system after it has been deployed into operation
- System impact assessment documentation

The organization should prepare technical documentation related to the responsible use of AI systems, covering the following:

- System failure management plans, fallback plans, system improvement or change plans, and plans for notifying customers and users

- System monitoring processes to ensure that the system operates as intended and within the defined scope
- Procedures to support system operation, such as monitoring and reviewing system and device logs
- Documentation defining the roles of personnel responsible for and overseeing system operation
- Documentation of system changes

The organization should establish procedures to support system changes, including communication to users. Technical documentation should be kept up to date and accurate and should be approved by the relevant management.

3.5.2.7) **AI system recording event logs**

The organization shall define the stages of the AI system life cycle where AI system event logs must be recorded. At a minimum, event logs shall be recorded for AI system operational activities.

Implementation Guidelines

The organization should require AI system logging to collect and record events occurring within AI systems. Logging should cover the following:

- The operation of AI system functions
- AI system performance, including both acceptable and unacceptable performance levels
- Recorded logs should include the date and time of AI system use, information on the data processed by the AI system, and outputs or results that are outside normal operation.

Logs should be retained for an appropriate period based on their intended use and in accordance with the organization's data retention policy and applicable legal requirements related to data retention.

3.6) Data for AI systems

Objective: To enable the organization to understand the role and impact of data in AI systems when applying, developing, providing, or using AI systems throughout the system life cycle.

3.6.1) Data for development and enhancement of AI system

The organization shall define, document, and implement data management processes related to the development and the use of AI systems.

Implementation Guidelines

Data management related to AI system development may cover the following topics:

- Management of privacy and security for the data in use
- Management of cybersecurity and safety threats
- Transparency and explainability of system operation, including data sources that can explain the linkage between system inputs and outputs

- Coverage of data used for system training
- Accuracy and completeness of data

3.6.2) Acquisition of data

The organization shall define and document details related to the acquisition and selection of data used in AI systems.

Implementation Guidelines

The organization may define the types of data used by AI systems from various data sources, depending on the scope and intended use of the organization's AI systems. Details of data acquisition may cover the following:

- Types of data used by the AI system
- Volume of data required
- How the data is obtained, such as internal data, purchased data, shared data, open data, or synthetic data
- Data characteristics, such as static data, streaming data, collected data, or computer-generated data
- Population-related data, such as age group, gender, income, education, employment, and marital status
- Data handling before use by the organization, such as alignment with privacy requirements and cybersecurity and information security requirements
- Rights related to the data, such as rights to use personal data and copyright
- Data descriptions or metadata
- Data provenance

3.6.3) Quality of data for AI systems

The organization shall define and document data quality requirements and shall regularly assess whether the data used for system development and the data used by the system conform to those documented quality requirements.

Implementation Guidelines

The quality of data used for the development and operation of AI systems has a significant impact on the accuracy of AI system outputs. ISO/IEC 25024 defines data quality as the degree to which the characteristics of data satisfy stated requirements when the data is used under specified conditions.

For AI systems using supervised machine learning and semi-supervised machine learning, the quality of training data, test data, and production data shall be defined, measured, and improved to an appropriate level. The data used shall be fit for the intended purpose of use.

The organization shall consider the impact of biased data on system performance and fairness and shall improve the model and data used as necessary to ensure that both performance and fairness remain at an acceptable level for use.

3.6.4) Data provenance

The organization shall define and document processes for recording the provenance of data used in the organization's AI systems throughout the data life cycle and AI system life cycle.

Implementation Guidelines

Data provenance records may cover data creation, data updates, data copying, data extraction, data validation, and data transfer. Data sharing and data transformation may also be considered part of data provenance, depending on factors related to data use, such as the content of the data, the context of data use, and other relevant factors. The organization should consider whether additional measures are required to verify data provenance.

3.6.5) Data preparation

The organization shall define and document the criteria used for data selection and the methods used to prepare data for use with AI systems.

Implementation Guidelines

Data used in AI systems typically requires preparation so that it can be effectively used by the AI system. Data that has not been properly prepared may cause the AI system to operate incorrectly.

Methods used to prepare and transform data for use in AI systems may include the following:

- Statistical exploration of the data to be used, such as distribution, mean, median, standard deviation, and range
- Data cleaning, such as correcting data errors
- Imputation of missing data
- Normalization of datasets, such as dividing all numeric values in the original dataset by 10
- Defining value ranges for datasets, such as specifying that values fall within a range of 1–10
- Naming variables
- Encoding datasets, such as converting categorical data into numerical codes

When preparing data for AI systems, the organization should document the criteria for data selection and the methods used for data preparation.

3.7) Information for interested parties of AI systems

Objective: To provide necessary information to interested parties of the organization's AI systems so that they understand the risks and both positive and negative impacts on the organization and relevant interested parties.

3.7.1) System documentation and information for users

The organization shall define and prepare the documentation and information necessary for users of AI systems.

Implementation Guidelines

Information related to AI systems includes technical details, instructions, or procedures for system use. AI systems should inform users that they are interacting with an AI system, depending on the context of use. Information generated as outputs from the AI system should also be communicated to users as appropriate.

Users should be informed of the purpose of system use, how the system operates, the expected benefits of the system, and any related harms or risks, where applicable.

Documentation provided to each group of stakeholders should be separated according to the nature of use and the information that each stakeholder group needs to know and understand before using the system.

Information required for users should cover the following:

- Purpose of system use
- Notification that the user is interacting with an AI system
- Methods for interacting with the AI system
- How and when to discontinue or avoid using the AI system
- Technical specifications of the system, including required system resources, system limitations, and system life span
- Human control and oversight
- Information on AI system accuracy and performance
- Relevant information from the AI system impact assessment, including associated benefits and harms
- System improvements and changes

3.7.2) External reporting

The organization shall provide the necessary systems and channels for stakeholders to report negative impacts of AI systems.

Implementation Guidelines

The organization should define channels for users or other external parties to report negative impacts of AI systems, in addition to reporting AI system issues or failures, such as system unavailability.

3.7.3) Communication of incidents

The organization shall define and document an incident communication plan for communicating with users of AI systems.

Implementation Guidelines

Incidents related to AI systems may be specific to AI systems, or may involve cybersecurity and information security incidents or personal data breaches.

The organization shall understand its roles and responsibilities to notify users and relevant stakeholders of such incidents. Notifications by the organization should cover the following:

- Types of incidents that require notification to relevant parties
- Required notification timelines
- Need to notify external competent authorities, such as relevant regulators
- Details of the information to be communicated

The organization may integrate incident reporting and response activities with organization-wide response activities. For example, where an incident involves cybersecurity and information security, existing mechanisms for responding to such incidents should be integrated with AI-related incident response into a unified process.

3.7.4) Information for interested parties

The organization shall define and document its duties, responsibilities, and obligations for reporting information related to AI systems to interested parties.

Implementation Guidelines

Information related to incidents and other matters shall be reported to relevant interested parties, such as customers, regulators, competent authorities, or other relevant parties, within the defined timeframe. The information to be reported should cover the following:

- Technical details of the system, including data used for system training, system testing, and the algorithm options used
- Risks related to the system
- Impact assessment results
- System logs and other information contained in the system

The organization should understand its roles and responsibilities for reporting and sharing information with appropriate competent authorities, including the applicable jurisdiction. For example, where an incident occurs, the organization may be required to report relevant information to competent legal authorities.

3.8) Use of AI systems

Objective: To ensure that the organization uses AI systems responsibly and in accordance with the organization's defined policies.

3.8.1) Processes for responsible use of AI systems

The organization shall define and document processes for the responsible use of AI systems.

Implementation Guidelines

The organization may consider whether to use a particular AI system, or whether a particular AI system should be developed internally or by an external service provider. The organization should clearly define standards for making such decisions to ensure correct and appropriate implementation.

The standard should cover the following:

- Approval for system development
- Costs of system development, including system maintenance costs
- Approval for procurement
- Relevant legal requirements
- Identification of AI capabilities requiring enhanced governance, such as facial recognition, biometric identification, surveillance technologies, emotion recognition, or other AI capabilities that may significantly affect individuals' rights, privacy, or freedoms
- Access to sensitive AI capabilities shall be limited to authorized personnel with legitimate business needs may access, develop, deploy, configure, or operate sensitive AI capabilities

3.8.2) Objectives for responsible use of AI system

The organization shall define and document objectives to provide guidance for the responsible use of AI systems.

Implementation Guidelines

Organizations operate in different contexts; therefore, expectations and objectives related to the responsible development and use of AI systems may differ.

Depending on the organizational context, the organization should identify objectives for the responsible development and use of AI systems that cover the following:

- Fairness and equity
- Accountability
- Transparency
- Explainability of system operation
- Trustworthiness
- Safety
- Continuity management to support situations that may cause operational disruption
- Privacy, cybersecurity, and information security
- System accessibility

Once these objectives have been defined, the organization should establish mechanisms to implement activities in alignment with those objectives.

The organization shall define objectives related to keeping humans in the loop for critical decisions through appropriate human control and oversight. The organization shall specify the stages of the system development life cycle where human control and oversight must be involved to ensure that critical decisions are not made solely by AI systems and that authorized personnel can intervene, override, or halt AI operations when necessary. Such objectives should include:

- Reviewing AI system outputs, including authority to override outputs or decisions made by the AI system
- Monitoring AI system performance, including the accuracy of AI system outputs
- Reporting concerns related to AI system outputs and potential impacts on relevant stakeholders
- Reporting concerns related to changes in AI system performance
- Determining whether automated decisions made by the AI system are appropriate

AI system impact assessments can provide initial information on which stages of the system development life cycle require human control and oversight. Personnel involved in human control and oversight should be informed of the AI system impact assessment report. These personnel should have sufficient knowledge and understanding of the documents related to the AI system so that they can perform their duties in accordance with the defined objectives for human control and oversight.

3.8.3) Intended use of the AI system

The organization shall assess whether the use of the AI system is consistent with the intended use and whether it aligns with the relevant system documentation.

Implementation Guidelines

AI systems should be deployed and used in accordance with the instructions, documentation, and manuals relevant to the AI system. When concerns arise from the use of an AI system, such as system outputs that may affect stakeholders, such information should be communicated to relevant parties, including external service providers.

The organization should retain logs and relevant documentation related to the use of AI systems to confirm whether the system is operating as intended, or to support communication of concerns when the system does not operate as expected. The retention period for logs and related documentation shall follow the organization's data retention policy and applicable legal requirements.

3.9) Third-party and customer relationships

Objective: To understand the organization's responsibilities, maintain primary accountability, and manage risks proportionately at the stages where external service providers are involved in the life cycle of the organization's AI systems.

3.9.1) Allocating responsibilities

The organization shall allocate responsibilities within the AI system life cycle to relevant parties, including the organization itself, partners, external service providers, and other relevant parties. In addition to process-based role allocation, the organization shall designate a clear Accountable Owner for the outcomes produced by each AI model or tool, to ensure that an individual or function can explain, review, and be accountable for the impacts arising from AI system outputs.

Implementation Guidelines

Within an AI system development life cycle, the organization shall clearly define and separate roles and responsibilities among the departments involved in the system, such as the department that provides data for the AI system, the department that prepares algorithms and models, the department that develops the system, and the department that uses the system.

Where the organization develops an AI system for an external party, the organization should follow the responsible system development practices defined in section 3.5. The organization shall provide the necessary documentation for that AI system to the external party for operation or further use.

Where personal data is processed in the use and/or development of AI systems, responsibilities shall be clearly separated between the processor and the personal data controller to protect data privacy. The organization may apply the measures defined in ISO/IEC 27701. Where the organization acts as the personal data controller and engages an external service provider that can access personal data under the organization's control for the use, development, operation, maintenance, or support of AI systems, that external service provider shall act as the personal data processor.

3.9.2) Suppliers

The organization shall define processes related to the use of services, products, or other deliverables from external service providers to ensure alignment with the organization's approach to responsible AI system development and use.

Implementation Guidelines

Organizations that develop or use AI systems may use external service providers in various ways, such as using datasets provided by suppliers, machine learning models or algorithms, or other system components such as software libraries.

The organization may consider different types of external service providers, their products or services, and the level of risk associated with each provider when selecting such providers.

The organization should document which components provided by external service providers, such as hardware, software, or other components, will be integrated into the organization's AI system.

Where the organization determines that an AI system or AI system component provided by an external service provider does not meet the organization's requirements, may affect individuals, groups of individuals, or society, or does not align with the organization's responsible practices, the organization should require the external service

provider to take corrective action. The organization may decide to work with the external service provider to achieve the organization's responsible AI objectives.

The organization should require external service providers to deliver appropriate and sufficient documentation related to the AI system (see sections 3.5.2.6 and 3.7.1).

3.9.3) Customers

The organization shall assess whether its approach to responsible AI system development and use considers the needs and expectations of the organization's customers.

Implementation Guidelines

The organization shall understand customer needs and expectations when it is required to deliver products or services related to AI systems to customers, where the organization acts as the service provider.

Such needs and expectations may be expressed as product or service requirements, contractual requirements, or terms of use. The organization may have different types of customers, and each type may have different needs and expectations.

The organization shall understand which responsibilities belong to the organization as the AI system service provider and which responsibilities belong to the customer as the service user, while continuing to meet the defined customer needs and expectations.

For example, the organization may identify risks associated with customer use of products or services. It is therefore responsible for defining approaches to manage those risks and communicating them to customers so that customers can take appropriate actions to manage such risks.

As another example of the organization's responsibility as a service provider, where an AI system provided by the organization is suitable for use within a defined scope, the limitations of use within that scope should be communicated to customers so that they can exercise appropriate caution and use the system within those limitations.

4) AI Usage Guidelines

4.1) Use of AI Technology for Organizational Operations

4.1.1) Users shall study each type of AI technology to understand its basic information, capabilities, benefits, risks, and limitations, so that users can appropriately and effectively apply AI technology in line with the objectives of each assigned task.

4.1.2) Users shall apply AI technology to support operations within the defined context as follows:

- Data analysis and report generation
- Writing scripts or programs
- Preparing draft letters or documents, such as memorandums, policies, or guidelines
- Providing initial recommendations or guidance for solving various issues
- Creating content for internal organizational communications
- Creating public relations materials
- Performing other tasks assigned by supervisors

The application of AI technology shall be limited to organizational missions and used solely for the benefit of the organization.

4.2) Prohibited Use of AI Technology

Although AI technology can support and improve users' operational efficiency in many ways, the use of AI technology must remain within an appropriate scope and must not cause harm to individuals, the organization, society, or the country. Therefore, the organization defines the following prohibited uses of AI technology:

- Do not use AI as a substitute for user decision-making in high-risk cases, such as legal decisions, financial decisions, or decisions that may affect a person's life, property, or rights.
- Do not access, deploy, configure, or use AI systems with sensitive capabilities, including facial recognition, biometric identification, surveillance technologies, or other AI capabilities and technology that involve the processing of high-risk or sensitive data, unless specifically authorized by the organization and approved in accordance with applicable legal, privacy, cybersecurity, and AI governance requirements.
- Do not use or disclose the organization's confidential information without approval from the Group CEO and CEO. Confidential information may include information contained in important internal documents or information that may affect the organization's operations.
- Do not use personal data without the consent of the data subject or use data in a manner that may violate the Personal Data Protection Act or other applicable laws.

- Do not use AI to create false information or content that may cause harm to individuals, the organization, or society, or that may manipulate or deceive individuals, exploit the vulnerabilities of individuals or groups of individuals, facilitate social scoring, or enable unauthorized biometric identification or surveillance. This includes, but is not limited to, as creating deepfakes, voice impersonation for fraud, or misleading images or videos.
- Do not use AI in a manner that violates good governance, integrity, ethics, morality, or that involves hidden or dishonest intent.
- Do not use AI to create content that infringes copyright or intellectual property rights, including reproducing, copying, or modifying content owned by other persons or organizations without permission.
- Do not use AI to create content that promotes discrimination based on race, religion, sex, age, disability, or social status, which may violate applicable laws and human rights principles.
- Do not use AI to perform any activity that may constitute a violation of laws, rules, regulations, requirements, announcements, orders, criteria, or other relevant obligations.
- Do not use AI in a manner that creates bias against individuals or groups of individuals, such as discriminatory treatment, unfair decisions, or biased outputs that have not been reviewed, or that results in subliminal or manipulative persuasion, exploitation of an individual's vulnerabilities, or social scoring.

4.3) Confidentiality and Personal Data Protection

The use of AI technology, particularly free-of-charge services, may create risks that information entered by users or interactions with the system may be accessed, recorded, or used to improve and develop system performance. Therefore, to prevent data leakage, infringement of individual rights, or damage to the organization, external parties, or relevant individuals, the organization shall keep humans in the loop when AI technology is used to process Confidential information or personal data by requiring appropriate human review, oversight, intervention and authorization before such information is used with AI systems. Users must exercise caution and comply with the following requirements:

- Do not use internal organizational information classified as “Confidential,” such as contracts, documents, or letters marked “Confidential,” together with AI technology. If such use is necessary, approval must be obtained from the Group CEO and CEO before using any Confidential information in all cases.
- Where AI technology must be used with personal data, developers and users shall notify the Group Chief Executive Officer (Group CEO) and Chief Executive Officer (CEO), and the personal data to be used shall have obtained consent from the data subject.
- If there are any questions regarding information security or legal requirements, users must consult with their supervisor, the Data Protection Officer (DPO), or relevant personnel before taking any action.

4.4) Information System Security When Using and Developing AI Technology

- Do not use information that may affect information system security, such as passwords, together with AI technology.
- Source code generated by AI technology must be reviewed before use, with careful consideration of correctness and vulnerability assessment.
- If a cybersecurity or information security incident arising from the use of AI technology is identified, users must immediately notify their supervisor through the appropriate reporting line and comply with the established procedures for cybersecurity and information security incident management.
- When using AI technology, users must ensure cybersecurity, information system security, data security, and other relevant security requirements.
- The organization may continuously monitor users' use of AI-related information technology to maintain the organization's cybersecurity and information security.

4.5) Reducing or Avoiding Bias and Discrimination Against Individuals or Groups of Individuals

Outputs generated from the development, use, and application of AI technology may create content containing negative views, bias, or discriminatory elements that may be widely disseminated and difficult to control. Such content may cause reputational or psychological harm to individuals and may create bias or discrimination against individuals or groups of individuals. Therefore, users must exercise caution and comply with the following requirements:

- Users must review content generated by AI technology before using it or publishing it to the public in order to reduce or avoid bias and unfair discrimination.
- Users must exercise caution when using AI technology for operations that may affect the rights of individuals or groups of individuals, or that may affect the principles of equality and human rights standards.

4.6) Duties and Responsibilities

The use of content generated by AI technology may cause negative impacts on individuals, departments, society, and the country, whether intentionally or unintentionally. The organization and users cannot deny responsibility for the consequences arising from such actions. Therefore, users and persons involved in the application of AI technology have the following duties and responsibilities:

- Users must inform their supervisors of the objectives, scope, and nature of AI-human involvement, and must notify their supervisors when using AI technology other than that specified by the organization for work purposes.
- Users must comply with the rules and methods for using AI technology.
- As defined in this policy, users must review AI-generated content before using or publishing it. Strict review is required, especially for content related to legal matters, financial information, and sensitive information. Users must consider the following matters:
  - Accuracy of content
  - Consequences of using or publishing content that may lead to unlawful acts, including copyright, trademark, or other intellectual property infringement
  - Equality and non-discrimination against individuals or groups of individuals
  - Confidentiality and personal data protection
  - Impacts on cybersecurity and information security, and risks that may arise from use
  - Other negative impacts that may occur to individuals, the organization, society, and the country
- Users must immediately report to their supervisors if errors or issues arise from the application of AI, including input or output issues that may negatively affect individuals, the organization, society, or the country, so that corrective measures can be taken promptly.
- Supervisors and users must continuously monitor, review, and evaluate the efficiency and effectiveness of AI technology use in order to improve working methods and select AI technology that is appropriate for work operations.
- AI-generated content should be distinctly labeled as “Generated by AI,” “Developed by AI,” or “Powered by AI” to promote transparency and prevent misunderstanding by recipients.
- AISC is responsible for reviewing and presenting to Group CEO and CEO the list of AI applications or services authorized for use within the organization, as appropriate to the level of use.

4.7) Respect for Intellectual Property Rights

- When using or publishing content generated by AI technology to the public, users must use only AI applications or services designated by the organization.
- When applying AI technology, users must exercise caution to avoid copyright, trademark, or other intellectual property infringement by ensuring that the generated content does not reproduce, copy, modify, or exploit works owned by others without permission, in order to prevent legal violations and potential disputes.

4.8) Training on the Application of AI Technology

The organization shall provide training for employees, workers, and personnel of the organization on the application of AI technology, including correct practices, ethical use, security, risks, technology limitations, and potential impacts, at least once a year.

4.9) Penalties for Non-Compliance

If any employee, worker, personnel, or contractor of the organization fails to comply with this document, such non-compliance may constitute misconduct and may result in disciplinary action in accordance with the organization's rules, regulations, announcements, or employment contract, depending on the circumstances and the user's relationship with the organization. The person may also be subject to penalties prescribed by applicable laws, subordinate legislation, rules, regulations, or relevant orders.

If users identify incorrect, inappropriate, or risky use of AI technology that may cause any damage, they must immediately report it to their supervisor or the responsible officer.

4.10) Examples of Do's and Don'ts for Using AI Technology

Do's	Don'ts
✓ Verify the accuracy of information before using it.	✗ Use information immediately without verifying its accuracy.
✓ Do not use the organization's confidential information with AI technology.	✗ Use the organization's confidential information with AI technology.
✓ Publish accurate and non-misleading information.	✗ Publish misinformation or disinformation.
✓ Always cite the source of information.	✗ Use information without citing its source.
✓ Avoid creating biased or discriminatory content.	✗ Create biased or discriminatory content.
✓ Use tools approved by the organization.	✗ Use tools that have not been approved by the organization.
✓ Avoid using content that may infringe copyright or intellectual property rights.	✗ Use content that may infringe copyright or intellectual property rights.
✓ Comply with the organization's policies and guidelines.	✗ Fail to comply with the organization's policies and guidelines.
✓ Avoid using AI technology in a manner that is unlawful or contrary to good governance, integrity, and ethics.	✗ Use AI technology in a manner that is unlawful or contrary to good governance, integrity, and ethics.

5) Normative references

The following documents are referenced in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document, including any amendments, applies.

- ISO/IEC 22989:2022 — International standard that defines terminology, conceptual frameworks, and standard definitions for artificial intelligence (AI) systems.
- ISO/IEC 25024:2015 — International standard on measurement of data quality, which is part of the SQuaRE (System and Software Quality Requirements and Evaluation) series. It is designed to assess and measure data accuracy and quality in computer systems using practical criteria such as completeness, accuracy, consistency, and credibility.

6) Terms and definitions

The following table defines key terms used in this document:

Term	Definition
Organization	WHA Group
WHA Group	WHA Corporation Public Company Limited and its subsidiaries, including associated companies over which the company has authority to control, direct, and define policies, procedures, standards, and other related documents.
Interested party	A person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.
Employee	Permanent employees, temporary employees, probationary employees, fixed-term employees, and special contract employees under WHA Group's work rules and employment conditions, including employees hired through contracting companies.
Management system	A set of interrelated or interacting elements of an organization used to establish policies, standards, objectives, and processes to achieve those objectives.
Policy	Intentions and direction of the organization, as formally expressed by top management.
Standard	A document, requirement, criterion, or specification developed by consensus to serve as a common reference for controlling the quality of operations, processes, or services so that they are consistent, secure, and interoperable, thereby increasing reliability and reducing duplication.
Risk	The effect of uncertainty, which may arise from various factors, such as: 1. Misinformation and disinformation: unintentionally false information that may mislead users (misinformation) and intentionally false information intended to mislead users (disinformation) may cause users to believe that the information is accurate and use it without considering the appropriateness and limitations of the technology. 2. Data privacy: the use of AI technology may affect data privacy, particularly when sensitive personal data is used. 3. Bias and discrimination: outputs generated from the application of AI technology may create content with negative views, bias, or discriminatory elements, which may cause reputational or psychological harm to individuals. 4. Information security: the use of AI technology may create information security risks, such as leakage of personal data or infringement of intellectual property rights. 5. Other negative impacts: the use of AI technology may cause negative impacts on individuals, the organization, society, and the country, such as generating factually incorrect content or dangerous or violent content.

Term	Definition
AI	Artificial Intelligence (AI) means technology that enables systems to learn, analyze, and make intelligent decisions in a human-like manner by using data and advanced algorithms.

- END OF DOCUMENT -